Mobile Security / Mobile Payments

Leslie K. Lambert
CISSP, CISM, CISA, CRISC, CIPP/US, CIPP/G
VP, Chief Information Security Officer
Juniper Networks

Professional Techniques - Session T23

MOBILE SECURITY / MOBILE PAYMENTS

Leslie K. Lambert CISSP, CISM, CISA, CRISC, CIPP/US, CIPP/G
VP, Chief Information Security Officer
Juniper Networks

October 16, 2012

MOBILE SECURITY / MOBILE PAYMENTS

- Agenda
  - Mobile Security
  - Mobile Payments

HIGH LEVEL
MOBILITY TRENDS

MOBILE DEVICE PROLIFERATION

500M+ smartphones and tablets shipped in 2011

Multiple OSes

WORKFORCE MOBILITY

Over 1 billion mobile users in 2011

Ubiquitous user access

CONSUMERIZATION OF IT AND BYOD

155% Malware increase in in 2011

36 billion worldwide app downloads predicted for 2012*

CLOUD AND MOBILITY SERVICES

Drives new opportunities – access and security services

**ABI Research, Mobile Application Market Data, April, 2012*

MOBILE DEVICE SECURITY MARKET GROWTH

$600 Million

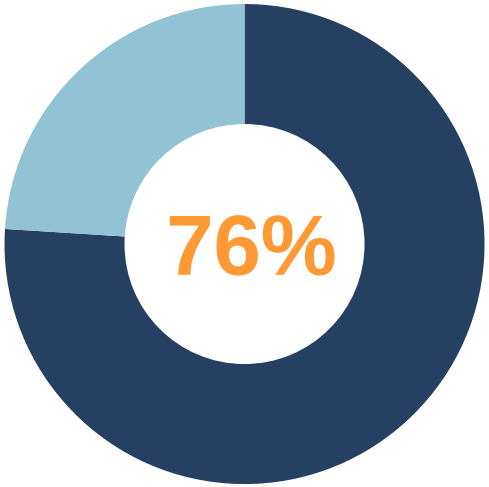
Mobile security client software sales, 2011*

$2.7 Billion

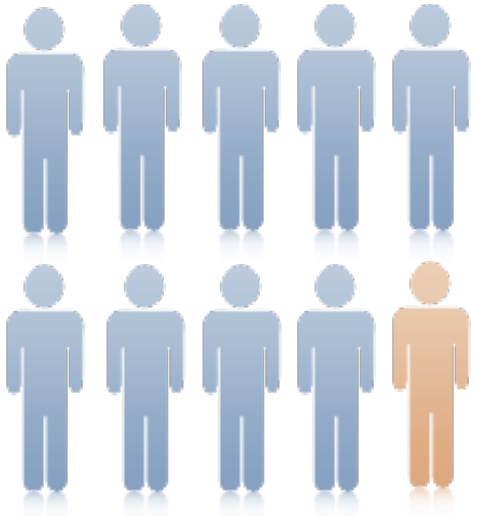
Projected mobile security client software sales, 2016*

**Source: Infonetics Research, Security Client Software report, April 2012*

MOBILE DEVICES ACCESS SENSITIVE DATA



Use their device to access sensitive data, such as online banking or personal medical information



9 out of 10 business users, say they access critical work information from their mobile device

Source: Juniper Networks' Trusted Mobility Index

PERSONAL MOBILE DEVICES IN THE ENTERPRISE

Source: Juniper Networks' Trusted Mobility Index

THE THREATS TO MOBILE DEVICES AND DATA

- **Malware –** Viruses, Worms, Trojans, Spyware
- **Direct Attack –** Attacking device interfaces, Network DoS, Malicious SMS
- **Loss and Theft –** Accessing sensitive data
- **Data Communication Interception –** Sniffing data as it is transmitted and received
- **Exploitation and Misconduct –** Online predators, pornography, inappropriate communications, data leakage

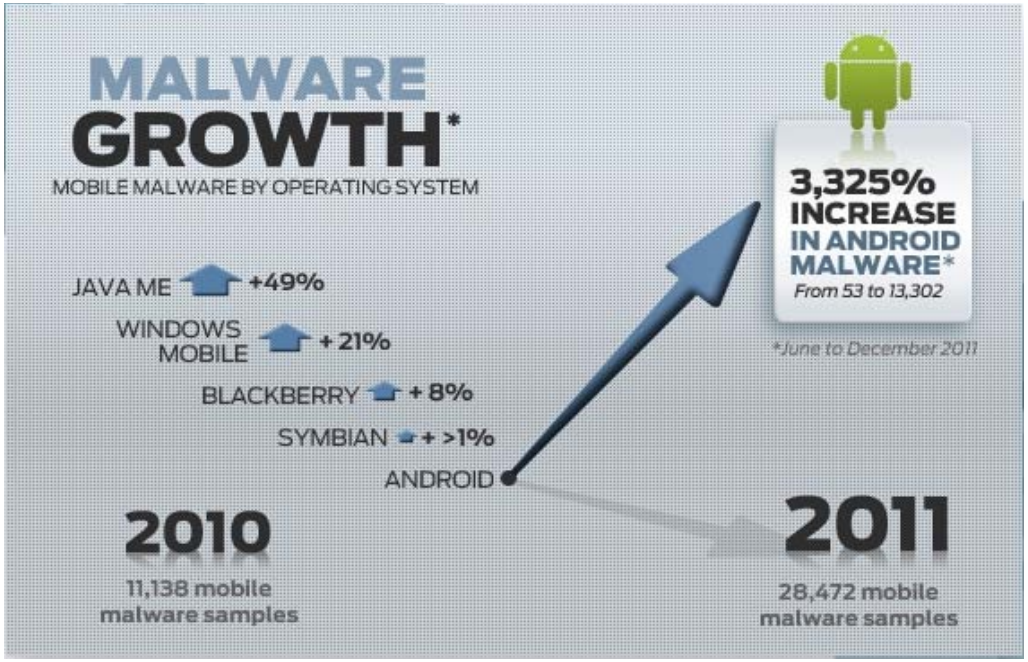
THERE IS MORE MALWARE THAN EVER BEFORE

46.9%

Android market share

In 2011, there were a record number of mobile malware attacks via device applications, particularly on the Google Android platform.

- Malware samples jumped **30%** in the first 3 months of 2012
- Instances of mobile spyware have **more than doubled** in the 1st quarter of 2012 ***alone***



Source: Juniper Networks' Mobile Threat Center 2011 Mobile Threats Report, February 2012

THREE PILLARS OF SECURING MOBILITY

SECURE CONNECTIVITY	MOBILE DEVICE SECURITY	MOBILE DEVICE MANAGEMENT AND CONTROL

THREE PILLARS OF SECURING MOBILITY

- **Secure Connectivity**
  - Ensuring secure access to corporate information assets from within an organization, or externally from the Internet.
  - Secure “tethering”
- **Mobile Device Security**
  - Provides enterprises with visibility into what’s on a smartphone and how it's being used, letting both IT and users better secure data and control costs without compromising privacy, even on employee-owned phones.
- **Mobile Device Management and Control**
  - Software that secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises.

ADVANCED TECHNOLOGIES ARE COMING…..

VIRTUALIZATION

ANTIVIRUS

NEAR FIELD COMMUNICATIONS

MONITOR AND CONTROL

 www.juniper.net

AND, ONE IN PARTICULAR…..

NEAR FIELD COMMUNICATIONS

http://www.nfc-forum.org

The Near Field Communication (NFC) Forum is a non-profit industry association that promotes the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs.

Becoming the de facto technology standard, peer-to-peer

Being found in next generation handsets / devices

Driving consumers to adopt more e-commerce and financial applications

PROXIMITY PAYMENTS

AND, DON'T FORGET THESE FUN DEVICES!

Square

intuit. Merchant Service

PayPal

 www.juniper.net

JUNIPER NETWORKS

NFC MOBILE CONTACTLESS SECURITY MECHANISMS

MOBILE PAYMENTS ….. DEFINITIONS …

Mobile as PAYMENT DEVICES to initiate payments by a consumer, at physical point-of-sale (POS) aka “proximity payments”, via e-commerce aka “remote payments”

Mobile as ACCEPTANCE DEVICES to accept payments by a merchant as the portable POS device

MOBILE WALLET – when the actual mobile device becomes the wallet, holds financial information (bank accounts, credit card numbers)

DIGITAL WALLET – not tethered to any specific device, exists in the cloud, accessible from a variety of devices in a number of ways

MOBILE PAYMENTS ….. CONSUMER BENEFITS

CONSUMER BENEFITS – enhanced shopping experience, unprecedented convenience, control of payment options, ability to research purchases and compare prices, share purchases with friends and family via social media, receive promotional opportunities, including digital coupons. Purchases can be made via proximity (physical store) or remote payments (e-commerce), conduct transactions wherever they take mobile devices . Post transaction convenience of having receipts stored on the mobile device for tracking and customer service purposes – no more paper receipts in your wallet!

MOBILE PAYMENTS ….. MERCHANT BENEFITS

MERCHANT BENEFITS – unrivaled opportunity to reach customers through multiple touch points simultaneously, where an electronic coupon delivered to a phone can be shared via social networking and used instantly or integrated directly into the digital wallet to be used in the next purchase, ability to determine the location of a consumer through geo-location functions to enable integrated marketing, incorporate privacy and security and customers will be receptive!

MOBILE PAYMENTS ….. WHAT ABOUT SECURITY AND COMPLIANCE?

Whenever a new technology is introduced, such as mobile payments, new challenges emerge.

The security and compliance challenges are protecting personal data that is either stored in or that flows through a mobile device (payment account numbers, PINs, security codes, passwords, etc.). NEED higher thresholds to assuage consumer concerns about security and privacy.

As with all cases in the past, addressing the threats are a shared responsibility of all stakeholders.

Fortunately, most of the security and compliance concerns associated with mobile payments are either identical or very similar to one already faced and addressed by the payment industry.

SECURITY OF MOBILE PROXIMITY PAYMENTS

PROXIMITY PAYMENTS – are based on the EMV standard and face the fewest security challenges. Use of an EMV-approved chip ensures that a mobile proximity payment delivers the same end-to-end security offered by a smartcard-enabled payment. In the case of proximity payments via barcodes or other means do represent new security and risk models that challenge the ability to deliver secure and cost-effective solutions. Standardization and integration must continue to be established – if not, will lead to attacks due to proliferation of "innovative" options. Need to implement defensive measures to secure the entire value chain of the mobile payment proximity payment ecosystem.

SECURITY OF MOBILE REMOTE PAYMENTS

REMOTE PAYMENTS – rely on software-based security that is susceptible to many threats due to the openness of the mobile platforms. Ability to execute all types of applications, from instant messaging to online banking and trading. This leads to increased viruses and malware targeting mobile platforms due to the increased adoption and penetration of mobile payments by consumers. Look for more advances in antivirus software for mobile platforms.

MOBILE PAYMENTS ….. STANDARDS THAT HELP!

PCI Security Standards Council™

PCI-DSS & PA-DSS – existing PCI-DSS's still govern the payments industry, all entities that process, transmit or store payment information must adhere to PCI-DSS. And, the Payment Application Data Security Standards (PA-DSS) applies to software applications used to accept payment data. The fundamental principles behind these standards are equally applicable to the mobile space, and likely these existing standards will be enhanced to incorporate new capabilities brought about the mobility and connectivity of mobile devices.

MOBILE PAYMENTS …. CONSUMER EDUCATION IS KEY

Mobile phones will carry more value than the cost of the phone itself and will need to be treated with extra caution. Treat mobile devices with same zeal as we currently do today with our wallets.

Use some form of password or passcode to access the payment application on the phone.

Only download mobile applications from trusted sources.

Ensure the text messages you receive from your financial institution originated from the correct phone number or short code.

Never share confidential or private information, especially if you did not initiate the communication. If in doubt, call your issuer.

Report to the financial institution immediately if your mobile device containing your financial information is lost or stolen.

THANK YOU !

everywhere

Leslie K. Lambert
CISSP, CISM, CISA, CRISC, CIPP/US, CIPP/G
VP, Chief Information Security Officer
Juniper Networks
llambert@juniper.net